Daily Open Source Infrastructure Report
22 August 2012

Top Stories

- An 80-car CSX train carrying coal derailed in downtown Ellicott City, Maryland, killing at least 2 people, crushing several vehicles in a parking lot, and dumping coal into a river. – *Washington Post* (See item **10**)
- An 11-mile stretch of the Mississippi River near Greenville, Mississippi, was closed August 20 to most vessel traffic because of low water levels, idling nearly 100 boats and barges. – *CNN* (See item **12**)
- AT&T Wireless partially disabled 16 cell phone towers after federal investigators found they were disrupting Oakland, California's police radio communications systems for months. – *San Francisco Chronicle* (See item **22**)
- Microsoft warned customers about the availability of the ChapCrack tool a researcher built to crack the VPN credentials for systems built on MS-CHAPv2 protocol. – *Threatpost* (See item **27**)
- Security researchers found a new trojan that tries to covers its tracks by crippling the victim's computer after stealing data. They said the malware was used in targeted attacks at specific individuals or firms, including at least one in the energy sector. – *Computerworld* (See item **29**)

Fast Jump Menu

Energy Sector

1. *August 21, Jamestown Sun* – (North Dakota) **Cleanup under way at site of oil well blowout.** Cleanup crews baled contaminated vegetation, scraped away affected soil, and power washed equipment August 20 after an oil well blowout south of Williston, North Dakota, that sprayed oil and salt water into nearby fields. Meanwhile, the Occupational Safety and Health Administration (OSHA) is investigating the death of a worker who was struck by a pickup as a worker drove it away from the spewing oil. The blowout, which sprayed 400 barrels of oil and 400 barrels of produced water used for hydraulic fracturing, is not believed to have contaminated water sources, said an environmental geologist with the North Dakota Department of Health Division of Water Quality. However, the cleanup contractor expanded the perimeter of the affected area because workers were seeing vegetation that was wilting and turning brown. The area that was most heavily affected is estimated to be about 30-40 acres. A mist of oil and salt water is believed to have extended no further than 1 mile in opposite directions of the well, affecting crop and pasture land. Workers estimated they recovered about 200 barrels of each fluid as they got control of the well. The incident occurred August 14.
   Source: http://www.jamestownsun.com/event/article/id/167503/

2. *August 21, Scranton Times-Tribune* – (Pennsylvania) **Possible vandalism investigated after chemical spill at gas well site.** State environmental regulators asked State police to help investigate a 100-gallon chemical spill at a natural gas well site in Susquehanna County, Pennsylvania, August 20, after bullet casings and a bullet were found near a broken glass tube that caused the leak. The spill of glycol was discovered by a worker at Cabot Oil and Gas Corp.'s Grosvenor well site in Dimock Township, a State Department of Environmental Protection spokeswoman said. The chemical was largely contained to the well pad but a heavy rain raised the risk of runoff, she said. Absorbent material and a vacuum truck were sent to the site to clean up the fluid. The broken tube was connected to a 500-gallon tank of glycol, which is used as part of the dehydration

process at the well site.
Source: http://thetimes-tribune.com/news/possible-vandalism-investigated-after-chemical-spill-at-gas-well-site-1.1361238

3. *August 20, White Plains Journal-News* – (New York) **State also faults Orange & Rockland Utilities in January gas blast.** A State Department of Public Service utility engineer's report on the January 16 natural gas explosion finds fault with the excavation contractor and Orange and Rockland Utilities (O&R) of New York. The agency's conclusion differs from that reached by the Rockland County District Attorney's Office, which accused only the contractor and his company, FGC Communications Inc., of crimes in relation to the blast at 52 Zarriello Lane that leveled one townhouse and damaged others. The massive explosion at the Village Fairground II housing complex also injured two West Haverstraw volunteer firefighters and two O&R employees. Based on the engineer's conclusions, the Public Service Commission (PSC) issued notices of probable violation to FGC and O&R June 15. Because of the PSC's citation against O&R, the contractor has recently filed a motion with the Rockland County Court to withdraw his guilty plea to a felony charge of first-degree reckless endangerment and his company's to a felony charge of first-degree assault. The contractor and his company entered the plea in May after negotiations between his lawyer and prosecutors.
Source: http://www.lohud.com/article/20120820/NEWS03/308200036/State-also-faults-O-R-utility-January-gas-blast?nclick_check=1

4. *August 20, Associated Press* – (Indiana) **BP recalls unleaded regular gas from Whiting.** BP alerted northwestern Indiana fuel distributors that it is recalling unleaded regular gasoline shipped from its Whiting, Indiana fuel storage terminal August 13-17. The company said August 20 it believes that fuel stored in a tank at the storage depot could cause hard starting, stalling, and other drivability issues. BP asked any customer whose vehicle has experienced those problems since August 13 to contact its customer hotline. BP said the fuel may have been purchased by motorists at BP and other retail outlets in the region. It said it is going through shipping records and contacting customers who may have loaded tanker trucks at the terminal during the affected period.
Source: http://www.wdtn.com/dpp/news/indiana/ap_indiana/BP-recalls-unleaded-regular-gas-from-Whiting_89792388

For more stories, see items **10**, **14**, and **29**

[Return to top]

Chemical Industry Sector

See items **2** and **11**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

Nothing to report

[Return to top]

Critical Manufacturing Sector

5. *August 20, Zacks Equity Research* – (International) **GM recalls full-size vans.** General Motors (GM) announced it would recall 10,315 units of full-size vans in 20 cold-weather U.S. States and in Canada because of fuel filler pipes that can rust and leak due to salt and chemicals used to clear snow from roads, Zacks Equity Research reported August 20. The recall covers Chevrolet Express and GMC Savana vans from the model years 2003 to 2004 with left-side cargo doors. GM will recall 9,389 vans in 20 U.S. States, including Connecticut, Delaware, Illinois, Indiana, Iowa, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, New Hampshire, New Jersey, New York, Ohio, Pennsylvania, Rhode Island, Vermont, West Virginia, and Wisconsin. GM revealed that salt and chemicals are prone to be trapped in a conduit that covers the fuel filler pipe, causing corrosion. As a result, gasoline may leak and lead to fire in the vehicles. GM has decided to fix the problem free of cost and will notify vehicle owners in October with the availability of required parts.
Source: http://community.nasdaq.com/News/2012-08/gm-recalls-fullsize-vans-analyst-blog.aspx?storyid=165447

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

6. *August 21, Cleveland Plain Dealer* – (Ohio) **Ponzi schemer pleads guilty to securities fraud, gets nine years.** A Ponzi schemer pleaded guilty August 20 in Cuyahoga County, Ohio, to 11 felony counts for bilking $60 million from nearly 900 investors in her failed Parma Heights Cornerstone Project. The woman ran an investment fraud scheme with her husband which involved a proposed multimillion-dollar retail and entertainment development that was never built. Prosecutors said that between 2003 and January 2005, she solicited family members, friends, and co-workers to invest in many development projects, including Cornerstone. She promised a high rate of return. A spokesman for the Ohio Department of Commerce said the scheme unraveled when the department's division of securities received a complaint from a family member who became suspicious after his mother was promised a 16 to 20 percent return on her investment. After the division investigated, it issued a cease-and-desist order against

the woman in May 2004 for selling unregistered promissory notes. She continued selling the notes, and the spokesman said the State then obtained a preliminary injunction against her. A few months later, she was found to have violated the preliminary injunction by continuing to sell securities without the court's permission. A receiver was then appointed to take possession of the couple's joint assets and of the woman's individual assets. The receiver recovered $10.5 million for the investors.
Source: http://www.cleveland.com/metro/index.ssf/2012/08/ponzi_schemer_joanne_schneider.html

7. *August 20, Reuters* – (National) **U.S. broker-dealer audit problems found in Ponzi scheme-inspired review.** Nearly 4 years after a broker-dealer admitted using his firm for a massive Ponzi scheme, a U.S. audit watchdog group says it is disturbed by problems that persist in audits of broker-dealers, including a failure to assess the risk of fraud, Reuters reported August 20. In its first report on inspections of broker-dealer auditors, the Public Company Accounting Oversight Board (PCAOB) said it found problems in all 23 audits it reviewed, including failure to test controls over customer funds. The problems were found during inspections of small broker-dealer audits conducted between October 2011 and February 2012. In 13 of the 23 audits the PCAOB checked, audit firms did not do enough to assess and respond to risks of material misstatements due to fraud, the board said. In two cases, audit firms helped prepare the financial statements they audited, a violation of Securities and Exchange Commission independence rules.
Source: http://www.reuters.com/article/2012/08/20/us-usa-audits-watchdog-idUSBRE87J0SO20120820

8. *August 20, CNNMoney* – (International) **U.S. seizes $150 million linked to Hezbollah money laundering.** Federal officials said August 20 that they seized $150 million as part of a crackdown on a money laundering scheme linked to the Lebanese militant group Hezbollah. The seizure came following a complaint filed in December 2011 alleging that the now-defunct Lebanese Canadian Bank laundered money for Hezbollah-controlled groups around the world. Officials said that between 2007 and 2011, Lebanese Canadian Bank and other financial institutions routed at least $329 million in proceeds from drug sales and other criminal activity to the United States, where this money bought used cars that were later sold in West Africa. These proceeds were then funneled back to Lebanon via Hezbollah-controlled channels. In September 2011, the majority of Lebanese Canadian Bank's assets were purchased by Societe Generale de Banque au Liban, another Lebanese bank. At least $150 million from that sale was being held in escrow in an account at Lebanon's Banque Libano FranÃ§aise, so U.S. officials seized an equivalent amount of money from a U.S. correspondent account of Banque Libano FranÃ§aise. Neither of the two banks were accused of wrongdoing.
Source: http://money.cnn.com/2012/08/20/news/world/feds-seize-hezbollah/index.html

9. *August 20, Dayton Daily News* – (Ohio) **Local credit card scam may be part of larger ring.** Two men who allegedly used personal information from consumers to create hundreds of fake credit and debit cards may be part of a larger ring, officials

said. Both men were indicted the week of August 20 in Warren County, Ohio, after they were arrested at the Franklin Walmart after they allegedly bought about $2,400 in merchandise and gift cards with credit and debit cards they created using stolen bank account information, according to a prosecutor. The prosecutor said the two allegedly obtained credit and debit card numbers and then used some sort of equipment to make the fake cards or at least used the bank data to obtain the cards. He said he was not certain where they obtained the numbers, but since many different banks were involved it did not appear to be an inside bank job. Alert cashiers apparently noticed the men were using many different bank cards at the self check-out to purchase mainly gift cards.
Source: http://www.daytondailynews.com/news/news/local-credit-card-scam-may-be-part-of-larger-ring/nRGHS/

[Return to top]

Transportation Sector

10. *August 21, Washington Post* – (Maryland) **Two killed as CSX train derails in Ellicott City overnight.** An 80-car CSX train carrying coal derailed in downtown Ellicott City, Maryland, late August 20 killing at least 2 people, authorities said. According to Howard County police, the derailment happened when an eastbound freight train came off the tracks of a rail bridge near Main Street. Police said 21 of the train's 80 cars derailed or overturned about 12 miles outside of Baltimore, falling off the tracks that run along the Patapsco River to the east. The train was en route from Grafton, West Virginia, to Baltimore. The 3,000-foot-long train was carrying 9,000 tons of coal and traveling at 25 miles per hour, officials said. They said one of the train cars fell off the bridge onto a county-owned lot beneath the tracks, crushing several parked vehicles. Cranes were brought in to remove the railcars from the vehicles. Crews were cleaning up the spilled coal, which also fell into the Patapsco River. The Associated Press reported about 100 pounds of coal spilled into a tributary of the river. A Maryland Department of the Environment spokesman said they were worried the coal would boost the acidity of the water or threaten aquatic life. Main Street and Frederick Road were closed from Ellicott City into Baltimore County.
Source: http://www.washingtonpost.com/blogs/post_now/post/two-killed-as-csx-train-derails-in-ellicott-city-overnight/2012/08/21/99d0a810-eb77-11e1-b811-09036bcb182b_blog.html

11. *August 21, WLNS 6 Lansing* – (Michigan) **One northbound and one southbound lane of 127 re-open.** One lane of southbound and one lane of northbound U.S. 127 were re-opened August 21, more than 1 day after a tanker truck flipped over early August 20 and leaked chemicals — specifically liquid asphalt — on the highway near Mason, Michigan. Crews said work on that side of 127 South would take weeks to remove all of the liquid asphalt from from ground and replace it with new soil. The accident happened between the Barnes and Kipp Road exits. A HAZMAT team, Michigan State Police, Michigan Department of Transportation, and Ingham County Sheriff's Office were all on scene. Police said the driver of the tanker was taken to a local hospital and treated for minor injuries.

Source: http://www.wlns.com/story/19317621/early-morning-accident-closes-both-lanes-of

12. *August 20, CNN* – (Mississippi) **Coast Guard halts traffic on low-water stretch of Mississippi.** An 11-mile stretch of the Mississippi River near Greenville, Mississippi, was closed August 20 to most vessel traffic because of low water levels, idling nearly 100 boats and barges, according to the U.S. Coast Guard. "We are allowing a limited number of vessels based on size" to attempt to pass, said a New Orleans-based Coast Guard spokesman adding that the closure was affecting 97 vessels and was halting northbound and southbound traffic. The same area near Greenville, which sees about 50 vessels pass on an average day, has been closed "intermittently" since August 12, when a vessel ran aground, he said. The Coast Guard and the U.S. Army Corps of Engineers have continued surveying the area and deemed it "dangerous for vessels to travel through," he said. The Corp also has being dredging in the area to deepen the channel and help navigation. A historic drought and excessive heat have reduced water levels and scorched wide sections of the U.S. Midwest. Flooding in 2011 may have worsened the situation on the Mississippi by leaving deposits of silt and debris in areas that would normally be clear.
Source: http://www.cnn.com/2012/08/20/us/mississippi-river-traffic/index.html?hpt=hp_t3

For more stories, see items **4** and **37**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

13. *August 21, Associated Press* – (California) **USDA eyes whether tainted beef entered food supply.** Federal regulators who shut down a central California slaughterhouse after receiving an animal welfare video were investigating August 21 whether beef from sick cows reached the human food supply. The video appears to show workers bungling the slaughter of cows struggling to walk and even stand. Under federal rules, sick animals cannot be slaughtered for human consumption. The investigation will determine whether sick cows were slaughtered and whether meat products from the company should be recalled, said a spokesman for the U.S. Department of Agriculture (USDA) Food Safety Inspection Service. The agency suspended operations August 20 at Central Valley Meat Co. in Hanford after receiving the video August 17 from the animal welfare group Compassion Over Killing. The footage shows animals bleeding and thrashing after being repeatedly shot in the head with a pneumatic gun in unsuccessful efforts to render them unconscious for slaughter. The USDA said investigators were trying to determine whether the cows in the video were just lame or

sick, which would render them unfit for human consumption. Compassion Over Killing said its undercover investigator was employed by the slaughterhouse and made the video over a 2-week period in June. Online USDA records show the company contracted to sell ground beef to USDA food programs.
Source: http://www.sacbee.com/2012/08/20/4742940/feds-close-central-valley-slaughterhouse.html#storylink=cpy

For another story, see item **1**

[Return to top]

Water Sector

14. *August 20, Utica Observer-Dispatch* – (New York) **Gas spill finds it way to Utica sewers, treatment plant.** The New York Department of Environmental Conservation (DEC) was investigating a gasoline spill that found its way into the sewer system and Utica, New York's wastewater treatment plant. The leak occurred sometime over the weekend of August 18 and was reported August 20. It was apparently due to an equipment failure at the Nice N Easy service station on Culver Avenue, according to a DEC spokesman. The Mohawk Valley Water Authority executive director said the gas spill would not affect drinking water in any way, and the sewer system is separate from the water supply. Officials said Nice N Easy hired a company to clean up the spill.
Source: http://www.uticaod.com/news/x1265469048/Gas-spill-finds-it-way-to-Utica-sewers-treatment-plant

For another story, see item **10**

[Return to top]

Public Health and Healthcare Sector

15. *August 21, Associated Press* – (Colorado) **715 whooping cough cases so far this year in Colo.** The Colorado health department said at least 715 cases of whooping cough have been reported through August 11 in the State so far in 2012. The department said the reported cases was far above the 5-year average of 158 cases typically reported by that time of year. The State health department executive director said August 20 that it is crucial for people who spend time around infants to be vaccinated against the respiratory disease. Health officials also are recommending the vaccine for pregnant women in the third or late second trimester and health care workers.
Source: http://www.aurorasentinel.com/news/715-whooping-cough-cases-so-far-this-year-in-colo/

[Return to top]

Government Facilities Sector

16. *August 21, Martinsburg Journal* – (West Virginia) **Man with armor, training rifle arrested.** A man wearing a ballistic vest and military camouflage, armed with a training rifle, two knives, and several unloaded magazines, was arrested August 20 after he was seen running in the area of two Martinsburg, West Virginia schools. The suspect, of Martinsburg, was charged with committing a terrorist act and wearing body armor while committing a felony offense following the incident, which occurred on the first day of school for Berkeley County students. "One of our primary concerns was that he was sighted in the general proximity or area of the high school on Bulldog Boulevard," a lieutenant said. "With him being in that proximity, we believed that he was causing a significant threat with his actions and his gestures by his own choosing." The suspect, who police said was a member of the military, later told police he was out running and jogging with his gear on. His current military status is under police investigation. The Martinsburg Police Department was assisted by the West Virginia State Police, the Loudoun County Sheriff's Office, the Martinsburg Fire Department and the Berkeley County Office of Homeland Security and Emergency Management in their investigation.
Source: http://www.journal-news.net/page/content.detail/id/583375/Man-with-armor--training-rifle-arrested.html?nav=5006

17. *August 20, U-T San Diego* – (California) **Suspect faces charges of threatening judge in El Cajon.** A Russian-born U.S. citizen accused of threatening a San Diego Sheriff's deputy and a judge at the El Cajon courthouse in California was being held in lieu of $1 million bail August 20 following his capture in Tijuana. He was detained August 16 by members of the Baja California Preventive Police in the Playas de Tijuana coastal enclave of San Antonio del Mar. Agents spotted him outside a residence and caught him after a brief chase, said an international liaison for the Baja California Public Safety Secretariat. He was turned over August 17 to members of the U.S. Marshals Service at the U.S.-Mexico border. The marshals delivered him to the San Diego Sheriff's Department, which had requested his capture. A news release from the Baja California Public Safety Secretariat described him as "a dangerous Russian terrorist" who "threatened to explode the installations of the court in San Diego...as well as kill judges and officials." The release stated that the threats led to the closing of the courthouse for 2 days. A San Diego Sheriff's spokeswoman said the man was arrested for "sending threatening emails" to the deputy and the judge.
Source: http://www.utsandiego.com/news/2012/aug/20/suspect-captured-in-tijuana-after-threatening-an-e/

18. *August 20, Government Security News* – (Virginia) **Man with alleged supremacist ties faces 10 years for illegal automatic weapon.** A man from Manassas, Virginia, arrested by the FBI's Washington Joint Terrorism Task Force (JTTF) in the spring pleaded guilty to illegal weapons charges August 17. The man faces a possible 10-year prison term when he is sentenced in November, according to the FBI. He came to law enforcement's attention when an informant saw his post on an Aryan Nation Web site indicating he was preparing to buy an AK-47 and have it modified to become fully automatic. In various online forums, he allegedly expressed hatred and support for

violence toward a number of political figures, according to the FBI. When FBI arrested him in the spring, the agency said he allegedly expressed support for violence against political figures, including the U.S. President and U.S. Attorney General. During his plea hearing August 17, he admitted providing a semi-automatic AK-47, along with $125, to an undercover law enforcement officer with the intent it be modified to become fully automatic. He was arrested May 30 by members of the JTTF after receiving the modified weapon from an undercover officer.
Source:
http://www.gsnmagazine.com/node/27038?c=law_enforcement_first_responders

19. *August 20, Iowa City Press-Citizen* – (Iowa) **Bomb threat cancels classes at Regina Monday.** Classes were canceled on the third day of school at Regina Catholic Education Center in Iowa City, Iowa, after a man called the high school August 20 and threatened to "blow up" the school. Bomb-sniffing dogs from the University of Iowa Department of Public Safety completed a 3-hour sweep of the elementary and junior/senior high school but found nothing suspicious, an Iowa City Police sergeant said. The president and CEO of Regina said the decision was immediately made to evacuate students and faculty after staff in the high school office received two calls from a man threatening to blow up the school. In accordance with school protocol, students and staff were taken to the school's safe zone, nearby First Presbyterian Church. Once it became evident the search of the school would take most of the day, parents were asked to pick up their children. The school sent an emergency email saying the campus was evacuated and all students were taken to the safe zone, according to a parent. A while later, she received a second email saying classes were canceled and she could pick up her children. Regina staff was allowed back inside the building later that afternoon. Investigators turned their attention to locating the man who made the phone calls.
Source: http://www.press-citizen.com/article/20120821/NEWS01/308210010/Bomb-threat-Regina-cancels-classes-day?nclick_check=1

[Return to top]

Emergency Services Sector

20. *August 21, Associated Press* – (North Carolina) **NC inmates sentenced to life could be released.** The North Carolina Court of Appeals ruled that a handful of inmates sentenced to life prison terms more than 30 years ago should be released because of a quirk in the law. In a 2-1 decision, the ruling August 21 applies to two men sentenced in the late 1970s to life terms for second-degree murder and second-degree burglary. The decision could set the stage for the release of at least 13 other inmates with similar cases. At the time, State law defined a life term as 80 years, but rules allowed for inmates to earn sentence reductions through classes or working while incarcerated. State lawyers argued the men should remain in prison until they die. The case is now likely to head to the North Carolina Supreme Court.
Source: http://www.myrtlebeachonline.com/2012/08/21/3011525/nc-inmates-sentenced-to-life-could.html

21. *August 20, Santa Rosa Press Democrat* – (California) **Glitch disrupts Santa Rosa 911 system.** Some emergency phone calls to the police department in Santa Rosa, California, went unanswered for an unknown amount of time August 20 after a blown circuit board disrupted service. The power failure stopped incoming phone lines, police radio system, and computer-aided dispatch system, said the police technical services manager. City staff scrambled to reroute all 9-1-1 calls to the Sonoma County Sheriff's Office dispatch center and officers began using a sheriff's radio channel. While calls to 9-1-1 from city phones were forwarded to the Sheriff's Office, some direct calls to the police dispatch number could not get through because the call-forwarding function was not working, the police technical services manager said. The circuit board was replaced by the end of August 20 and regular service was restored.
Source: http://www.pressdemocrat.com/article/20120820/ARTICLES/120829956

22. *August 20, San Francisco Chronicle* – (California) **Oakland police radio culprit: cell towers.** The San Francisco Chronicle reported August 20 that Oakland, California officials said they and federal investigators have discovered a major source of disruption to the city's police radio communications system: Interference from cell phone towers. Specifically, officials said, cell phone towers operated by AT&T Wireless have been interfering with the city's public safety communications frequency and causing radio failures among police and firefighters on city streets. AT&T, notified by the city of the problem the week of August 13, is cooperating and has partially disabled 16 towers. The towers constantly interfered with the radios, but the problems became particularly pronounced when a police car was within a quarter to a half mile of a tower, said Oakland's public safety systems adviser. The city's public safety radio communications system has suffered repeated failures. Officers routinely have been unable to connect to dispatchers or to communicate with other officers. In addition, the radios do not work in hundreds of buildings, including the basement of Oakland police headquarters.
Source: http://www.sfgate.com/crime/article/Oakland-police-radio-culprit-cell-towers-3802585.php

23. *August 20, Firehouse.com News* – (Texas) **Thousands worth of equipment stolen from Texas FD.** The Leroy-Axtell Volunteer Fire Department in Texas is without equipment and gear worth close to $3,000 after their station was broken into the weekend of August 18. In total, a bunker coat, fire helmet, EMS airway bag, EMS trauma bag, and an AED are missing. Two other helmets, pants, and a pair of boots were recovered after they apparently fell off of the thief's truck. The fire chief said the loss will take the department longer to arrive on the scene and it could take the department a month to replace the equipment. The McLennan County Sheriff's Office is currently investigating the break-in.
Source: http://www.firehouse.com/news/10761534/thousands-worth-of-equipment-stolen-from-texas-fd

24. *August 20, Asheville Citizen-Times* – (North Carolina) **Report issued in Asheville firefighter's death.** Failure to follow an "air management doctrine" and standard procedures for fighting a high-rise fire likely contributed to the death of an Asheville, North Carolina fire captain in 2011, a report from a federal agency that investigated the

fire concluded. The report from the National Institute for Occupational Safety and Health, released to the public August 20, also suggested the captain may have shown signs of carbon monoxide poisoning before he ran out of air inside the building. The captain died and nine firefighters were hurt in the fire July 28, 2011. The arson fire remains under investigation. The Asheville fire chief said his department immediately began looking at ways to improve standard procedures following the fire and already implemented some recommendations included in the report. The department will release its own internal report to City Council's public safety committee August 27 and to the full Council August 28.
Source: http://www.citizen-times.com/article/20120821/NEWS/308210011/Report-lists-Bowen-death-factors?odyssey=mod|newswell|text|Frontpage|s&nclick_check=1

[Return to top]

Information Technology Sector

25. *August 21, The H* – (International) **Apache Server 2.4.3 fixes over fifty bugs and two security holes.** The Apache Software Foundation released version 2.4.3 of the Apache HTTP Server, fixing over 50 bugs and closing 2 security holes. The two vulnerabilities are present in the mod_proxy_aip, mod_proxy_http, and mod_negotiation modules. The two gaps were listed as CVE-2012-3502 and CVE-2012-2687, but there is little information available on the actual problems. The first bug happens with mod_proxy_sjp and mod_proxy_http in the backend when a connection is closing which "could lead to privacy issues due to a response mixup." The second problem, in mod_negotiation, concerns a possible cross-site scripting (XSS) where untrusted users are uploading files; it is fixed by escaping file names.
Source: http://www.h-online.com/security/news/item/Apache-Server-2-4-3-fixes-over-fifty-bugs-and-two-security-holes-1672035.html

26. *August 21, The H* – (International) **Apple Remote Desktop update fixes VNC security problem.** Apple released version 3.6.1 of its Apple Remote Desktop application for remotely managing Mac OS X systems to fix an information disclosure vulnerability. According to Apple, the security update addresses a serious problem when connecting to third-party VNC servers that may result in data not being encrypted when the "Encrypt all network data" setting is enabled. Additionally, when this happens, no warning is produced to alert users that their connection may be insecure.
Source: http://www.h-online.com/security/news/item/Apple-Remote-Desktop-update-fixes-VNC-security-problem-1671129.html

27. *August 20, Threatpost* – (International) **Microsoft warns users about ChapCrack tool availability.** Microsoft is warning customers about the availability of the ChapCrack tool a researcher built to crack the VPN credentials for systems built on MS-CHAPv2 protocol. The company said that while it is unaware of any active attacks using the tool, customers can protect themselves by implementing protected extensible authentication protocol or changing to a more secure VPN tunnel. In its advisory, Microsoft says that while the ChapCrack tool does not take advantage of a security vulnerability, it still represents a risk to users. "An attacker who successfully exploited these cryptographic

weaknesses could obtain user credentials. Those credentials could then be re-used to authenticate the attacker to network resources, and the attacker could take any action that the user could take on that network resource," the company said in its advisory on ChapCrack.
Source: http://threatpost.com/en_us/blogs/microsoft-warns-users-about-chapcrack-tool-availability-082012

28. *August 20, Threatpost* – (International) **Own the email, own the person.** For attackers looking to take control of a victim's online presence, there is no better place to start than the target's email account. New research done by a member of IOActive shows just how simple it can be to get control of a target's email account, and from there, everything else. The researcher started a research project to see how easily he could access volunteers' email accounts. Targeting friends and family members who agreed to the experiment, the researcher found that with just the data he gathered online from Facebook and other sites, he had little trouble accessing the target's inboxes. The best mechanism for obtaining access, in most cases, was the password-reset function on various sites and email services
Source: http://threatpost.com/en_us/blogs/own-email-own-person-082012

29. *August 17, Computerworld* – (International) **Shamoon malware cripples Windows PCs to cover tracks.** A new trojan tries to covers its tracks by crippling the victim's computer after stealing data, a security researcher said August 17. Dubbed "Shamoon" by most antivirus companies, the malware has been used in targeted attacks aimed at specific individuals or firms, including at least one in the energy sector. According to security company Seculert, Shamoon relies on a one-two punch, first taking control of a system connected to the Internet before spreading to other PCs on an organization's network. The second stage overwrites files and the Master Boot Record (MBR) of the machine. The latter makes the PC unbootable. Seculert and other security companies, including Kaspersky Lab and Symantec, have not yet figured out what kind of data Shamoon is looking for, then stealing. They assume that because the malware uses a second infected system to communicate with a hacker-controlled command-and-control (C&C) server, Shamoon is copying files from pillaged PCs and sending that information to its masters. Malware rarely destroys files or wipes the MBR. Most threats try to work quietly to avoid detection as long as possible. Crippling a computer only brings unwanted attention. "Threats with such destructive payloads are unusual and are not typical of targeted attacks," Symantec said August 16. Since a list of overwritten files is transmitted to the C&C server, Seculert's CTO speculated that Shamoon's makers wanted to "know what and how much got wiped."
Source:
http://www.computerworld.com/s/article/9230359/Shamoon_malware_cripples_Windows_PCs_to_cover_tracks?taxonomyId=82

For another story, see item **36**

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: https://www.it-isac.org

[Return to top]

Communications Sector

30. *August 20, WCBD 2 Mount Pleasant* – (South Carolina) **SCE&G equipment failure interrupts WCBD-TV newscast.** WCBD 2 Mount Pleasant in South Carolina experienced broadcast interruptions August 20 during its evening newscast due to an SCE&G equipment failure. WCBD is located in the utility service area affected by the power outage. The outage caused WCBD to periodically lose news content, audio, and lights during its newscast. A SCE&G spokesperson said power crews were working to fix the equipment and restore electricity to area homes and businesses that were impacted. There was no report on what caused the SCE&G equipment to fail.
Source: http://www2.counton2.com/news/2012/aug/20/power-failure-interrupts-newscast-ar-4377509/

For another story, see item **22**

[Return to top]

Commercial Facilities Sector

31. *August 21, WCMH 4 Columbus* – (Ohio) **36 units destroyed in north side apartment fire.** Firefighters battled a large two-alarm apartment building fire on the north side of Columbus, Ohio, August 20. Fire crews arriving on the scene found heavy fire coming from a unit of the apartment building, however, they said it appeared the fire started in a room used for storing bulk trash. Investigators are treating the fire as suspicious in nature. Firefighters said the fire destroyed 36 units and caused more than $800,000 in damages.
Source: http://www2.nbc4i.com/news/2012/aug/20/6/columbus-firefighters-battling-2nd-alarm-apartment-ar-1143678/

32. *August 21, KXTV 10 Sacramento* – (California) **Fire, hazmat crews battle 3-alarm fire at Stockton warehouse.** A fire at a warehouse in the Mormon Slough area of Stockton, California, August 20 burned two businesses and destroyed another. Firefighters on scene stated crews were called to the warehouse and found the building engulfed in flames. One of the three businesses inside that belonged to a general contractor contained paint which leaked during the blaze, firefighters said. HAZMAT crews were called to the scene to help with containment and cleanup efforts. The general contractor's business was destroyed in the fire. A nursery was also housed in

the warehouse, but firefighters did not state how badly that business was burned.
Source: http://www.news10.net/news/article/205873/2/Fire-Hazmat-crews-battle-3-alarm-fire-at-Stockton-warehouse

33. *August 21, El Paso Times* – (Texas) **18 people hospitalized after falling ill at West El Paso call center.** Eighteen people were taken to 2 area hospitals and more than 200 were evacuated from a call center in west El Paso, Texas, after being exposed to a non-toxic chemical August 20. Although hospital officials could not disclose the condition of the patients, treatment consisted of decontamination of the eyes and lungs, a health spokesman said. Fire and emergency crews responded to reports of a strange odor at Redcats USA. An outside vendor was testing the fire suppression system and accidentally set it off, releasing the chemical potassium salt, a dry non-toxic extinguishing agent said a spokesman for El Paso Fire Department. Exposure to the chemical caused irritation in the eyes and discomfort in the respiratory systems of the patients, the health spokesman said. The company is an online and catalog retailer of plus-size clothes, home and lifestyle products, sporting goods, and outdoor gear, according to its Web site.
Source: http://www.lcsun-news.com/las_cruces-news/ci_21358232/18-people-hospitalized-after-falling-ill-at-west

34. *August 21, Associated Press* – (Kentucky) **Police injure suspect during shootout at Walmart.** Kentucky State Police investigated a shootout between a suspect and a central Kentucky officer that happened in the parking lot of a Walmart as bystanders watched. Police said the incident began August 20 when a shoplifting suspect was detained at the store in Stanford. Police said the suspect pulled a gun and ran out of the store into the parking lot where he fired twice at a city police officer, who shot back. A police spokesman told WKYT 27 Lexington that people were traveling in and out of the area, which also has a fast-food restaurant, a gas station, and a drug store. However, police said no one was injured except the suspect, who suffered non-life-threatening wounds.
Source: http://www.wlky.com/news/local-news/kentucky-news/Police-injure-suspect-during-shootout-at-Walmart/-/9718420/16207452/-/nxslorz/-/index.html

35. *August 20, Associated Press* – (Washington, D.C.) **Guard commits suicide at Smithsonian art museum.** Officials said they evacuated the Smithsonian's Hirshhorn Museum and Sculpture Garden in Washington, D.C., when a security guard was found dead of a self-inflicted gunshot wound. Smithsonian Institution officials said the guard shot himself with his service revolver August 20 in a locker room in the basement level of the building. Officials said no one from the public witnessed the shooting, and no one else was injured. The museum on the National Mall was evacuated and remained closed for the rest of the day. The Hirshhorn is the Smithsonian's modern art museum. Washington, D.C. police are investigating.
Source:
http://www.google.com/hostednews/ap/article/ALeqM5hxFMBCrNgwmBNINXSZdxwPTPhxNQ?docId=ada2cf19ad43451d900fa19fd295bf8a

36. *August 20, Softpedia* – (International) **Company promises to address vulnerability in hotel room locks.** At the 2012 Black Hat USA security conference, a security researcher demonstrated how a vulnerability in Onity keycard locks — used by hotels worldwide for millions of room doors — could be leveraged to open a door, Softpedia reported August 20. The company recently promised to address the issue. To mitigate the attacks described by the researcher, Onity provided several solutions. One would be to provide customers with a mechanical cap, along with a security TORX screw, to cover up the port the expert used to connect his own device to the lock's portable programmer. The researcher answered said this free solution would prove effective because it considerably increases the time needed to hack the lock. However, he stressed this may not work for locks from the ADVANCE series. The second solution is a firmware upgrade on the locks from the ADVANCE and the HT series. This measure involves the replacement of the entire control board and it would require customers to pay a nominal fee. Since the costs of the security upgrade would not be insignificant and would be handled by the hotels, the researcher expressed fears that many owners might choose not to implement the new systems, leaving their customers exposed.
Source: http://news.softpedia.com/news/Company-Promises-to-Address-Vulnerability-in-Hotel-Room-Locks-287089.shtml

For more stories, see items **3** and **10**

[Return to top]

National Monuments and Icons Sector

37. *August 21, Associated Press* – (California) **Fire update: Ponderosa Fire grows to 16,000 acres.** A huge wildfire sparked by lightning burned to the edge of three small, northern California towns, threatening thousands of homes as residents sought safety miles away at an emergency shelter, the Associated Press reported August 21. More than 1,800 firefighters were battling the Ponderosa Fire in rugged, densely forested terrain in Tehama and Shasta counties as it threatened 3,500 homes in the towns of Manton, Shingletown, and Viola. The fire destroyed 7 homes while blackening 23 square miles. It was 30 percent contained as of August 20. The fire forced the closure of Highway 44 and other roads, with Cal-Fire also issuing evacuation warnings in the area of Highway 36 at Oasis Springs Road to Lassen Lodge. As of August 20, the Mill Fire was 55 percent contained. The Chips Fire burning in the Plumas and Lassen National Forests grew to nearly 51,000 acres. Containment of that blaze was at 37 percent.
Source: http://newstalk1290.wordpress.com/2012/08/21/fire-update-ponderosa-fire-grows-to-16000-acres/

38. *August 20, Salt Lake Tribune* – (Utah) **Two wildfires burn in northern Utah, no structures threatened.** Fire crews continued to battle two wildfires in northern Utah August 20. Campgrounds and trails in Diamond Fork in Utah County remained closed August 20 as the Red Ledges fire grew eight-fold in 24 hours. The blaze burned 2,400 acres on Red Mountain by August 20, and was at zero percent containment. It started

August 19 and forced the evacuation of campers and hikers in the area. The fire was suspected to be human-caused, possibly by someone using a chain saw, officials said. Meanwhile, crews were fighting the Whiskey fire, which was burning about 5 miles southeast of Heber City in the Whiskey Springs area near Daniels Canyon. The fire burned about 272 acres August 20 and did not grow during the day. As of nightfall, it was 30 percent contained, said a fire spokesman. Also August 20, fire officials said Jordanelle Reservoir was reopened to water craft. It was closed to all water traffic August 19 as crews battled a nearby wildfire.
Source: http://www.sltrib.com/sltrib/news/54727533-78/fire-blaze-monday-sunday.html.csp

39. *August 20, Associated Press* – (Washington) **Fire in central Washington 57 percent contained.** Fire crews reached 57 percent containment August 20 on a central Washington wildfire that burned dozens of homes. Crews worked to gain the upper hand on several wildfires burning east of the Cascade Mountains in advance of predicted thunderstorms that could bring lightning and possibly new fires. The Taylor Bridge Fire east of Cle Elum burned across more than 36 square miles. About 1,000 firefighters were fighting the blaze. August 20, some of them conducted controlled burns of potential fuel. Meanwhile, a new, lightning-caused fire near Wenatchee was reported close to full containment. The Keane Ranch Fire burned 1 square mile.
Source: http://www.oregonlive.com/pacific-northwest-news/index.ssf/2012/08/fire_in_central_washington_57.html

[Return to top]

Dams Sector

40. *August 21, Chennai Hindu* – (International) **Yeleru canal breaches.** The Vemulapudi bund of Yeleru canal, one of the major sources that supply water to the city of Visakhapatnam in India, breached early August 20. The breach was 6 meters wide. The superintendent engineer (SE) of water supply initiated measures for plugging the breach. Earth moving machines and about 100 workers were pressed into service to prevent wastage of water. The breach was to be plugged that night and water flow stabilized. The SE said there would be no disruption in water supply August 21.
Source: http://www.thehindu.com/news/cities/Visakhapatnam/article3802649.ece

41. *August 20, WBNS 10 Columbus* – (Ohio) **Dam removal under way.** The demolition process began at the Fifth Avenue dam on the Olentangy River, WBNS 10 Columbus reported August 20. About a third of the dam will be removed to recreate a more natural-flowing stream. The Columbus Dispatch reported construction will also remove a drowning hazard that claimed the life of a man 4 years ago. The project will cost about $7 million. It should conclude by the week of September 3.
Source: http://www.10tv.com/content/stories/2012/08/20/columbus-dam-removal-under-way.html

[Return to top]

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2314
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer